PUBLIC UTILITIES COMMISSION
505 VAN NESS AVENUE
SAN FRANCISCO, CA 94102-3298

June 26, 2017

GI-2017-03-GRS-38-01C

Mr. David A. Weber, President and CEO (Dave.Weber@nwnatural.com)
Gill Ranch Storage
220 NW 2nd Avenue
Portland, OR 97209

SUBJECT: General Order 112 Gas Inspection of the Gill Ranch Storage Leak Survey, Patrolling and Control Management (CRM) Program and Records.

Dear Mr. Weber:

On behalf of the Safety and Enforcement Division (SED) of the California Public Utilities Commission, Paul Penney, Dmitriy Lysak and Molla Mohammad Ali conducted a General Order 112[1] inspection of Gill Ranch Storage (GRS) from March 20-24, 2017. The inspection included a review of GRS's Control Room Management (CRM) Program (Plan) and associated records, and Leak Survey and Patrolling records.

All items noted in this audit letter are recommendations from GRS's CRM Plan. As noted in the recommendations section of the inspection letter, GRS has accepted the recommended changes identified during the on-site inspection, and incorporated them into the CRM written program. In addition to these recommendations, additional recommendations were identified in a post-inspection review of GRS's CRM Plan.

Within 30 days of your receipt of this letter, please provide a written response indicating the measures taken by GRS to address the additional recommendations noted in the Summary.

If you have any questions, please contact Paul Penney at (415) 703-1817 or by email at paul.penney@cpuc.ca.gov.

Sincerely,

Kenneth A. Bruno
Program Manager
Gas Safety and Reliability Branch
Safety and Enforcement District

Enclosure: Summary of Inspection Findings

cc: Karl Leger, RegSafe (Karl.Leger@regsafe.com)
Todd Thomas, GRS (Tthomas.nwngs@nwnatural.com)
Dennis Lee, SED (Dennis.Lee@cpuc.ca.gov)

[1] General Order 112-F was adopted by the Commission on June 25, 2015 via Decision 15-06-044, with an effective date of January 1, 2017.

SUMMARY OF INSPECTION FINDINGS

I. Violations

No violations were noted during the audit.

II. Concerns/Recommendations

All recommendations are related to GRS's CRM written program. GRS has accepted the following recommendations and incorporated them into the written program. PHMSA's CRM protocol questions, SED staff recommendations, GRS's updated language and SED's conclusions are identified below.

Protocol Question B4-4:

When a controller is unable to continue or assume responsibility for any reason, does the shift hand-over procedure include alternative shift hand-over actions that specifically address this situation?

- If the incoming controller is late arriving, procedures should address the responsibilities of the current controller and/or management to address the issue.
- If controllers are permitted to find their own replacement among available controller staff, control room supervisors/managers should still be accountable for Hours of Service (HOS) requirements and limitations.
- Operator's procedures should provide a mechanism for an on-shift controller (or a controller due to come on shift) to alert management that he/she is unable or unfit for duty, because of illness, fatigue, car trouble or other issues.

SED Recommendation:

Add language to address bullet number one.

GRS's Updated Language:

GRS added the language (highlighted in yellow) to Section 15.5.1.1 (Shift Turnover Meeting) to address bullet one.

A turnover meeting will be conducted to brief incoming pipeline controllers on the status of current operations even if no unusual event occurred during the previous shift. If the same controller is to return for the next shift, a shift turnover meeting will be conducted to ensure no critical information has been forgotten. This turnover meeting shall occur at the console/desk and will also clearly indicate when the incoming pipeline controllers have taken over the responsibility of the operations. This may include electronic or hard copy checklists and/or signed documents such as a logbook.

GRS personnel shall complete the shift turnover log when performing the shift turnover meeting. This form shall be used to ensure that all required information is communicated to the incoming controller. This form shall not be used as a substitution for conversation. The record shall identify the incoming and outgoing controllers along with the topics covered during the meeting and the date and time of the shift turnover.

In the event an incoming controller is late or unable to assume responsibility for any reason, the outgoing controller may be asked to perform a holdover shift. As long as the

controller's hours are in compliance with this program's Fatigue Mitigation Program and the proper Hours of Service requirements are met.

SED's Conclusion:
The revised language meets the intent of this recommendation.

Protocol Question E1-2:
Does the review of safety-related alarms account for different alarm designs and all alarm types/priorities?

- Operator must ensure soft (software calculated or "synthetic") alarms are accurate and can be identified by the controller.
- Adequate procedures must be in place to explain the administrative controls for the disabling of safety -related alarms.
- FAQ E.12. Alarm priorities used by the operator should differentiate alarm importance. Too many alarm priorities could lead to confusion and inconsistent response to alarms.
- In evaluating whether alarms support safe operations, operators should account for type of alarm used, e.g., visual alarms are more likely to go unnoticed than alarms that are both audible and visual. Make a notation of the types of alarm used.

If there are differences in alarm design based on alarm priority, the operator should be able to explain the rationale for the chosen approach and its effect on ensuring controllers recognize and handle alarms efficiently.

SED Recommendation:
Add language to reflect the fact that alarm priorities do not dictate which alarms are handled first.

GRS's Updated Language:
GRS added the following language (highlighted in yellow) to Section 15.8.3.5 (Alarm Prioritization).

There are three different alarm priorities.
• A priority of 1 is a safety/critical alarm and will be indicated red on the alarm banner.
• A priority of 2 is a warning alarm and will be indicated yellow on the alarm banner.
• A priority of 3 is a notification and will be indicated purple on the alarm banner.

Currently, alarm priorities are not used to prioritize the controller's response. Therefore, all alarm priorities (at this time) are considered safety-related alarms and are addressed based on operating configuration (e.g. withdrawal, injection) and type (e.g. pressure, flow, temperature, level) instead of priority group (e.g. 1, 2, 3). Controller's use their experience and the alarm conditions to set priorities and responses.

SED's Conclusion:
The revised language meets the intent of this recommendation.

Protocol Question E2-2:
Does the operator's alarm management plan include a procedure for promptly correcting identified problems and for returning these points to service?

- Operator should analyze problems to identify recurring or chronic issues that are not getting corrected promptly enough.
- FAQ E.14.

SED Recommendation:
Add specific language for how "identified problems" are documented (i.e., SAP).

GRS's Updated Language:
GRS included the following language (highlighted in yellow) to the CRM Manual, Section 15.8.6.5 (Correction of Identified Problems Including Inaccurate or Malfunctioning Alarms). Please note the editorial comments below, which are highlighted in red.

All identified problems including inaccurate or malfunctioning alarms must be reported as soon as practicable, but no later than by the end of the shift. The notification process includes a request for alarm maintenance and/or repairs. Notification of inaccurate/ malfunctioning alarms ~~and~~ shall be documented and communicated to the on-coming controller as part of the shift change procedure. Alarm repair requests shall be made as soon as practicable, but no later than the end of shift. The timing/urgency of the repair request must be made with an understanding of the operational risks associated with the inaccurate/malfunctioning alarm.

Identified problems are addressed:

1. In daily stand-up meetings. Inaccurate or malfunctioning alarms are recorded in the log book and reviewed at shift change and (as needed) discussed during the daily stand-up meeting. Repairs/ replacements are performed by the Process Technician as soon as practicable so long as it does not impact the operational safety of the pipeline system. Records of repairs and replacements are scheduled and maintained in either SAP or the Operators Log Book.
2. Emergency repair/ replacement of inaccurate of malfunctioning alarms are reviewed either as they occur or at shift change and in the daily stand-up meetings. The Process Technician performs these repairs/ replacements As Soon As Possible. These events may require GRS to either shut-in all or part of the pipeline system or curtail operations until the repair/ replacement can be completed. Records of repair and replacements are scheduled and maintained in ~~either~~ SAP.

Prior to the implementation of a change to an alarm set-point value, the value must be verified as accurate. See 15.8.3.1 Rationalization. Prior to the implementation of a change of a set-point value in the SCADA system, the value must be verified as accurate. See 15.8.3.1 Rationalization. All alarm points shall be promptly returned to service and/or appropriate safe guards implemented to assure the safe operation of the pipeline system.

SED's Conclusion:
The revised language meets the intent of this recommendation.

Protocol Question E3-2:
Have procedures been established to clearly address how and to what degree controllers can change alarm limits or setpoints, or inhibit alarms, or take point's off-scan?

- FAQ E.17 Controllers should not be able to change setpoints associated with critical maximum or minimum safety limits. However, operators may choose to allow controllers to change other mid-level alarm setpoints used for operational purposes.
- Changed setpoints should be verified as having the correct valve before implementation.
- Verification should explicitly check setpoint values currently in the SCADA system, not just check a listing of what the setpoints should be.
  Controllers should have convenient access to a listing of all alarm limits and alarm descriptions.

SED Recommendation:
Add language to the GRS Control Room Management (CRM) plan to reflect bullet one above.

GRS's Updated Language:
GRS added the following language (highlighted in yellow) to Section 15.8.8.6 (SCADA Alarm Set-Point Values and Description Review).

Safety related alarm set-point values and descriptions shall be reviewed for accuracy each calendar year, at intervals not exceeding 15 months. The review shall ensure that:
• Alarms descriptions are clearly understood by controllers;
• Alarm descriptions are consistent in format; i.e. alarms from the same location should have the same location coding;
• The pressure and flow alarm set-points are correct for each alarm priority; and
• Alarm set-points in the field are consistent with those in the control room.

Note: Offsets may exist between the field and control room alarm setpoints to alert controllers to take action prior to critical field thresholds are breached.

Controllers are encouraged to take part in the review and may be solicited for input when choosing or editing the text of the alarm descriptors.

Controllers are not able to change and/or edit alarm set points. Should Controllers feel that an alarm should be adjusted it should be brought up at the daily stand-up meeting or communicated to the plant superintendent via email. Such requests are discussed and reviewed with all controllers and other subject matter experts prior to any changes being implemented. These reviews may be conducted as part of a meeting (e.g. stand-up meeting) or thru a more formal review such as a Management of Change request.

SED's Conclusion:
The revised language meets the intent of bullet one.

Protocol Question:
N/A

SED Recommendation:
Add an appendix that includes the forms that are used as part of the CRM program.

GRS's Update:
GRS responded to the recommendation as follows.

This section has been added to the end of the Control Room Management Plan. The Forms appendix is now located in section 15.12.5 – Forms. This includes all pertinent forms for the Control Room Management Program in one central location as suggested.

SED's Conclusion:
The appendix was verified to be in the latest revision of the CRM Plan.

Additional Recommendations:
The following additional recommendations are made after a post-audit review of GRS's Control Room Management Program (Plan), which was received after the audit. PHMSA's CRM protocol questions and SED staff recommendations are identified below.

Protocol Question B4-5:
Has the operator established adequate procedures for occasions when the console is left temporarily unattended for any reason?

- FAQ B.04. Depending on an operator's specific system operations, a particular control room may not have to be staffed by controllers, full time. The operator's procedures should include an explanation of when and how the pipeline is operated when the control room is unattended.
- Such procedures should include special provisions for shift change realizing that face-to-face communications between the departing and arriving controllers may not occur.

SED Recommendation:
For bullet two, SED staff recommends that GRS add language to the plan to address the unlikely situation for when face-to-face communications are not possible.

Protocol Question C2-3:
Has the operator established and implemented an adequate procedure for the thoroughness of the point-to-point verification?

- FAQ C.02 and C.06.
- The procedure must define the extent of verification to include physical location of device, data value or status, any alarm settings, and to assure that any test signals are injected at the actual device in the field.
- The verification procedure must include a requirement to check a representative sampling of impacted displays. FAQ C.03.
- FAQ C.05. If the verification process includes partial simulation, the operator must establish a procedure to define when simulation should be used in point-to-point verification.
- FAQ C.05. If the verification process includes partial simulation, the operator must establish a procedure to define what type(s) of simulation is/are applicable for specific instruments and equipment during point-to-point verification.

SED Recommendation:
Point-to-Point verification documentation is covered in Section 15.6.3.2, and the point-to-point verification form is in Section 15.12.5.5. SED staff recommends adding a physical location description field per bullet number two into both Section 15.6.3.2 and the form.

Protocol Question C2-4:

Has the operator established and implemented an adequate procedure for defining when the point-to-point verification must be completed?

- FAQ C.20. Point-to-point verification must be completed in a timely manner. Those data points already being used by controllers should be verified the same day a verification process became necessary.
- FAQ C.20. Those data points being added or checked out as a part of a major system enhancement or replacement should be verified before those data points are turned over to controllers for use.

SED Recommendation:
Per bullet one and FAQ C.20, SED staff recommends GRS add expectations to the CRM plan for when point-to-point verification must be completed.

Protocol Question C4-2:
Has the operator adequately defined the use of the backup SCADA system for development work?

- Operators should be very cautious about using a back-up system for development work, since prototyping could inadvertently reach the on-line system
- Operators should implement the guidance in Advisory Bulletin (ADB–03–09) "Potential Service Disruptions in Supervisory Control and Data Acquisition Systems" dated December 23, 2003 (68 FR 74289) and Advisory Bulletin (ADB-99-03), "Potential Service Interruptions in Supervisory Control and Data Acquisition Systems" dated July 16, 1999 (64 FR 38501).
- If a separate development SCADA server is being used, it should be isolated from the on-line environment.

SED Recommendation:
SED staff recommends that GRS add an overview description of the development workstation to the CRM Program document, including how the workstation is isolated from the on-line SCADA system. For example, Section 15.8.3.8 (Alarm Design and Implementation- Updates and/ or changes) is one possible section for adding this paragraph.

Protocol Question C4-4:
Does the testing verify that there are adequate procedures in place for decision-making and internal communications to successfully implement a transition from primary SCADA to backup SCADA, and back to primary SCADA.

- Procedure and test must address the circumstances under which the back-up SCADA system is to be activated, so that the test adequately simulates conditions under which the backup SCADA system will be used.
- Procedures must clearly define who is responsible for making the decision to transfer pipeline control to the backup SCADA system, and restoring control from backup to normal operations. This decision-making process must be a part of the annual testing.
- Procedures must address and test internal communications to implement transfer of control to backup SCADA systems, as well as to transfer control back to the primary SCADA system.

- Procedure must provide guidelines for evaluating the causes/circumstances of a primary SCADA system or communications outage before making the decision to transfer to backup SCADA, and how those causes/circumstances impact operations using backup SCADA systems.
- Any redundant SCADA for primary control room must be tested.
- Any SCADA at a backup control room must be tested.
- An adequate procedure should be in place to explain when it is safe to put the primary SCADA system back on-line.

SED Recommendation:
SED staff recommends that GRS add language to the CRM Program to address bullet number seven.

Protocol Question E1-3:
Does the review of safety-related alarms account for individual-specific controller qualification and performance?

- If there are differences in display object characteristics, formats, or colors from one console to another, those differences must be explicitly addressed in controller training and accounted for in alarm management plan.
- Controller qualification tests should evaluate the ability of controllers to accurately perceive SCADA display object characteristics (e.g., color, shape, text) that indicate safety related alarms used in the operator's SCADA system.
- If a controller is not able to clearly discern all individual colors used, the operator may consider incorporating alternatives to achieve an equivalent level of SCADA display understanding for all controllers.
- Requirements for operator qualification are addressed in 195.505(b) and 192.805(b).

SED Recommendation:
SED staff recommends that GRS add language to address this topic. If the contractor who performs training and testing incorporates the elements identified in this protocol question, please reference that in the CRM Plan.

Protocol Question E4-1:
Has the operator established and implemented procedures to review the alarm management plan at least once each calendar year, but at intervals not exceeding 15 months, in order to determine the effectiveness of the plan?

- Procedure must identify the interval and method for reviewing alarm management plan.
- Procedure must identify factors and criteria used to measure alarm management effectiveness.
- Results of the review must be documented, even if the review determines that no changes were warranted.
- FAQ E.16. Procedure must provide for addressing findings in a timely manner. In addition, the operator's alarm management plan should include provisions to analyze its specific deficiencies to identify root cause, common cause, trends, etc., that are indicative of systemic deficiencies that need to be identified and corrected.
- Alarm management effectiveness metrics might include number (volume) of alarms, clarity of alarm descriptions, how alarms are displayed or presented to controllers,

etc. Effectiveness could include, but not necessarily mean reduction in number of alarms or reduction in alarm volume.

SED Recommendation:
SED staff recommends GRS include a reference in Section 15.8.8.3 to the document used in accomplishing the review and gauging the effectiveness of the alarm management plan.

Protocol Question H5-1:
Has the operator established a list of pipeline operating setups that are periodically (but infrequently) used?

- "Periodically but infrequently" means operational setups that are repeatedly used at quarterly or greater intervals.
- Operational setups occurring more frequently than quarterly would not be "infrequent."
- FAQ H.01. The operator must establish a list of applicable setups, including but not limited to: startup, shutdown, shut-in, purge, ILI tool runs, station or line section bypass, system configurations involving mainline block valve closure, operating pressure restrictions, stopple fittings, slack line conditions, occasional delivery lateral operation, line reversals (reversing direction of flow), combining pipelines through valving to run in common versus split, bleed valve operations, power loss failure modes, seasonal set-ups, etc.

SED Recommendation:
With regard to bullet three, SED staff recommends GRS include a list of infrequently used setups, such as startup, shutdown (i.e., when a SCADA communications failure occurs) and the configuration used during ILI tool runs.